UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
V.	)	Crim. No. 15-cr-10271-WGY
ALEX LEVIN	)	

DEFENDANT'S MOTION FOR DISCOVERY

The defendant, Alex Levin, moves this Court to order the government to produce the following requested discovery. As grounds, the defendant states that the requested information is material and relevant to the preparation of his defense, and that he cannot properly prepare for trial without access to it.

Case Background

The defendant has been indicted for a single count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). This case stems from the government's investigation of a child pornography website, Playpen. Playpen came to the government's attention in August 2014, and was reportedly the largest child pornography website it had ever uncovered. Playpen operated on an anonymous network known as "Tor." Unlike the ordinary internet, communications on Tor are bounced through a network of computers around the world, which in turn disguises the user's actual Internet Protocol ("IP") address. Consequently, it is impossible to trace these communications back to the original computer, which allows Tor users to operate in anonymity.

The government seized control of Playpen in 2015. In order to circumvent the

anonymous nature of the Tor network, the government obtained a search warrant that allowed it to install a piece of software called a Network Investigative Technique ("NIT") on the website. The NIT surreptitiously transmitted a computer code to any computer that accessed Playpen. The user's computer would then send identifying information to a government-controlled computer located in the Eastern District of Virginia, including its IP address, operating system, host name, username, and Media Access Control ("CMAC") address. An IP address linked to the defendant's home was one that was supposedly collected by the NIT. Consequently, the government obtained a search warrant for his home, which led to the discovery of files believed to contain child pornography on one of his laptops.

Requested Discovery

Defense counsel sent a letter to the government requesting discovery on April 18, 2018. A second letter with additional discovery requests was sent on August 3, 2018. These letters have been appended with this motion as Exhibits 1 and 2. The government has not responded to either of the defendant's discovery requests. The defendant now moves the Court to order the government to furnish the defendant with the items of discovery listed in each of the letters.

Argument

Federal Rule of Criminal Procedure 16 provides that upon a defendant's request, the government must permit the defendant to inspect and copy evidence in its possession so long as it is material to preparing the defense. Fed. R. Crim. P 16(a)(1)(E)(i). A showing of materiality requires an indication that disclosure of the information sought

would allow the defendant to significantly alter the quantum of proof in his favor. *United States v. Goris*, 876 F.3d 40, 45 (1st Cir. 2017), citing *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975). This indication may take many forms such as "uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993).

The defendant seeks information and materials related to the NIT. The gravamen of the government's allegations against the defendant stem from information it claims to have obtained via the NIT. It follows that the software's accuracy is of paramount importance to the defense. The defendant has retained Joseph Nicholls, an expert in digital forensic services, to assist with the preparation of this case. Mr. Nicholls has assisted with the discovery requests, and has prepared an affidavit delineating the need for the discovery. *See* Exhibit 3. Mr. Nicholls, who has 40 years of experience in the field of digital forensic examination, is unable to completely assess the accuracy of the government's claims without access to this discovery. Instead, the defendant is in the unenviable position of having to rely upon the government's assertions that the NIT operated correctly, without being able to independently verify this claim.

In the three and a half years that this case has been pending, the defendant has not received any discovery related to the NIT. As detailed in Mr. Nicholls' affidavit, failure to provide the requested materials makes it impossible to assess whether the defendant's computer did in fact access Playpen. This discovery is critical to Mr. Nicholl's forensic examination, so that he can compare the information contained on the defendant's computer with the information purportedly collected by the government. The defendant

cannot properly prepare a defense without access to the requested items.

The requested discovery meets the standard outlined in *Lloyd*. Undoubtedly, allowing the defense expert to review the materials upon which the government relies in making its assertions would assist in rebutting the prosecution's case. Without being permitted to do so, the defendant is unable to adequately address the government's claims at trial. Moreover, access to this information will assist Mr. Nicholls in preparing to testify. It will also likely reveal admissible evidence in the form of additional information about how and why the government came to identify the defendant.

This request is not without precedent. In *United States v. Budziak*, the Ninth Circuit vacated the defendant's conviction for possession of child pornography where he was denied access to materials related to the software the government used to access files on his computer. 697 F.3d 1105, 1112-13 (9th Cir. 2012). At trial, the government presented evidence describing the software and the FBI's use of the software. *Id.* at 1112. The defendant was denied access to material that would have allowed him to "pursue a more effective examination" of the government's software expert. *Id.* The Court found that this was error. *Id.* Citing a Third Circuit opinion, the Court stated, "'[a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately.'" *Id.*, quoting *United States v. Liebert*, 519 F.2d 542, 547-48 (3d Cir. 1975). Moreover:

> In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless . . . criminal defendants should not have to rely solely on the

> government's word that further discovery is unnecessary. This is especially so where, as here, a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to the software.

Id. at 1112-13.

The same rationale that the Ninth Circuit applied in *Budziak* should also apply to the case at bar. Mr. Nicholls' affidavit makes clear that the requested discovery is material to the defense. Without it, the defendant must simply defer to the government's assertions. It is impossible for the defendant to fully prepare to cross examine the government's experts or to deliver a sufficient rebuttal without the opportunity to review the evidence that forms the basis for a substantial portion of the allegations.

At least one District Court has ordered the government to produce the NIT's source code. Just as in this case, the defendant in *United States v. Michaud*, Western District of Washington No. 3:15-cr-05351-RJB, moved for production of the NIT source code. The government declined to turn over the discovery, arguing that the defendant failed to establish materiality and that, even if the code was discoverable, the law enforcement privilege applied. Judge Bryan of the Western District Court of Washington rejected these arguments and ordered the code to be produced. *See* Exhibit 4, *United States v. Michaud*, Transcript of February 17, 2016 Hearing Re: Motion to Compel. Following oral arguments on the motion to compel, Judge Bryan stated:

> Well, first I am satisfied that the defense has shown materiality here to preparing the defense. I don't need to discuss that in depth, in my view. I think the papers speak for themselves. And it may be a blind alley, but we won't know until the defense can look at the details of what was done.
>
> So far as the privilege is concerned, what has been presented is nothing

> more than a showing that disclosure could possibly lead to harmful consequences . . . [T]he government said . . . that disclosure could possibly lead to a variety of harmful consequences. It is my opinion that the protective order in place is sufficient to protect this information, and it is my judgment that the motion should be granted. The material requested should be submitted, but under the terms of the protective order in place.
>
> . . . The government hacked into a whole lot of computers on the strength of a very questionable search warrant. I ruled on the admissibility of that in what I considered to be a very narrow ruling . . . [I]t comes down to a simple thing. You say you caught me by the use of computer hacking, so how do you do it? A fair question. And the government should respond under seal and under the protective order, but the government should respond and say here's how we did it.

Exhibit 4 at 17-19.

Judge Bryan's reasoning in *Michaud* applies with equal force to this case. The government identified the defendant on the basis of technology to which the defendant has not been provided access. The government must be required to produce this discovery, reveal its methods, and allow the defendant to conduct an independent review and test the government's claims.

Conclusion

For the foregoing reasons, the defendant moves that this motion be allowed and the government be ordered to furnish the requested discovery to the defendant.

ALEX LEVIN
By his attorneys,

CARNEY & ASSOCIATES

J. W. Carney, Jr.

J. W. Carney, Jr.
B.B.O. # 074760

Daniel J. Gaudet
B.B.O. # 688120

20 Park Plaza, Suite 1405
Boston, MA 02116
617-933-0350
JCarney@CARNEYdefense.com

December 14, 2018

Certificate of Service

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on or before the above date.

J. W. Carney, Jr.

J. W. Carney, Jr.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
V.	)	Crim. No. 15-cr-10271-WGY
ALEX LEVIN	)	

AFFIDAVIT IN SUPPORT OF DEFENDANT'S MOTION FOR DISCOVERY

I, J. W. Carney, Jr., state that the facts contained in the attached motion are true to the best of my information and belief.

Signed under the penalties of perjury.

J. W. Carney, Jr.

J. W. Carney, Jr.

December 14, 2018